EXHIBIT

D

United States

New User | Log-In | Contact UPS | The UPS Store Search Sub

My UPS Shipping Tracking Freight Locations Support UPS Solutions

Tracking Number Track

Log-In for additional tracking details.

Other Tracking Options

Tracking Detail

Like 1.4m Share Print Help A A A

1Z51708E0263740194

Updated: 03/19/2015 5:10 P.M. Eastern Time

Delivered

Delivered On:
Friday, 03/06/2015 at 1:35 P.M.

Left At:
Office

Signed By:
PATRICK

Proof of Delivery

Request Status Updates »

What time will your package be delivered to your home? Get FREE approximate Delivery Windows on most UPS packages.

Continue

I am already a UPS My Choice® Member

UPS Live Chat

Launch Chat

Shipping Information

To:
BOYNTON BEACH, FL, US

Shipped By

UPS 2nd Day Air®

Shipment Progress

What's This?

Location	Date	Local Time	Activity
Riviera Beach, FL, United States	03/06/2015	1:35 P.M.	Delivered
	03/06/2015	7:15 A.M.	Out For Delivery
	03/06/2015	5:55 A.M.	Arrival Scan
Hialeah, FL, United States	03/06/2015	4:39 A.M.	Departure Scan
Hialeah, FL, United States	03/05/2015	11:34 P.M.	Arrival Scan
Miami, FL, United States	03/05/2015	11:30 P.M.	Departure Scan
	03/05/2015	10:33 P.M.	Arrival Scan
Louisville, KY, United States	03/05/2015	8:02 P.M.	Departure Scan
	03/05/2015	12:44 P.M.	Arrival Scan
Kokomo, IN, United States	03/05/2015	9:02 A.M.	Departure Scan
	03/05/2015	6:18 A.M.	Arrival Scan
Wyoming, MI, United States	03/05/2015	2:18 A.M.	Departure Scan
Wyoming, MI, United States	03/04/2015	8:34 P.M.	Origin Scan
United States	03/04/2015	6:20 P.M.	Order Processed: Ready for UPS

Additional Information

Shipped/Billed On:	03/04/2015
Type:	Package
Weight:	3.30 lbs

Subscribe to UPS E-mail: Enter e-mail address Sign Up » iew Examples Site Feedback

Contact UPS
Browse Online Support
E-mail UPS
Live Chat
Call Customer Service

Support
Get Started
Register
Open a Shipping Account
Change Your Delivery

Solutions for:
Healthcare
Small Business
High Tech
More...

Other UPS Sites:
Select a website

Follow us:

UPS UNITED PROBLEM SOLVERS®

Home About UPS Site Guide Investors Careers Pressroom UPS Global UPS Mobile UPS Blog

Service Terms and Conditions Website Terms of Use Privacy Notice Your California Privacy Rights Protect Against Fraud

SUPPLEMENTAL DECLARATION OF PATRICK PAIGE

I, PATRICK PAIGE, DO HEREBY DECLARE:

1. I am over the age of eighteen (18) and otherwise competent to make this declaration. The facts stated in this declaration are based upon my personal knowledge.

2. I was a police officer from 1989 until 2011 for the Palm Beach County Sherriff's Department. From 2000-2011, I was a detective in the computer crimes unit.

3. As a detective in the computer crimes unit, I investigated internet child pornography and computer crime cases.

4. I have conducted forensic computer examinations for:

(a) Broward County Sheriff's Office (BSO);

(b) Federal Bureau of Investigation (FBI);

(c) U.S. Customs and Border Protection (CBP);

(d) Florida Department of Law Enforcement (FDLE);

(e) U.S. Secret Service;

(f) Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); and

(g) Various municipalities in the jurisdiction of Palm Beach County.

5. I was assigned to a police unit working in conjunction with TLO Corp., which is a private company.

6. When I worked with TLO Corp., I supervised the other detectives assigned to the unit, which consisted of six online investigators and two computer forensic examiners.

7. With regard to my experience investigating child pornography cases, I supervised police officers whose responsibility it was to establish a successful TCP/IP connection with

persons who were sending pornographic images of children or other illegal content over the Internet using peer-to-peer file sharing programs.

8. I have taken over 400 hours of courses designed to teach people how to investigate computers.

9. Also, while working from 2003-2011 for Guidance Software, the makers of EnCase, I have taught over 375 hours of courses in computer forensics ranging from beginner to advanced levels.

10. I have had students in my courses from various government branches, including: (a) sheriff's offices; (b) FBI agents; (c) ATF agents; (d) agents from the Central Intelligence Agency, and (e) individuals from other branches of government and the private sector.

11. After leaving the Palm Beach County Sherriff's office, I founded Computer Forensics, LLC, where I am currently employed.

12. I have received the following awards and commendations:

(a) 1991 – Deputy of the Year, awarded by the 100 Men's Club of Boca Raton & Rotary Club.

(b) 1997 – Deputy of the Month for June.

(c) 2001 – Detective of the Month for October.

(d) 2002 – Outstanding Law Enforcement Officer of the Year, awarded by the United States Justice Department for work in the *U.S. vs. Jerrold Levy* case.

(e) 2003 – U.S. Customs Service Unit Commendation Citation Award for computer forensic work in Operation Hamlet. Operation Hamlet was one of the largest rings in the history of U.S. Customs of individuals who were molesting their own children, and transmitting the images and video via the Internet.

(f) 2005 – Detective of the Month for December.

(g) 2007 – Outstanding Law Enforcement Officer of the Year, awarded by the United States Justice Department for work in the *U.S. vs. Jimmy Oliver* case.

(h) 2008 – Letter of Commendation issued by the FBI for outstanding computer forensic work in the *U.S. vs. Frank Grasso* case.

13. I have testified as a fact and expert witness on numerous occasions in the field of computer forensics in both trial-level and appellate proceedings before state, federal, and military courts in Florida, California, Indiana, New Jersey, New York, and Pennsylvania.

14. No court has ever refused to accept my testimony on the basis that I was not an expert in computer forensics. My skill set and my reputation are my most important assets in my current position with Computer Forensics, LLC.

15. The offenders' IP addresses, as well as the dates and times of the illegal transmission were recorded.

16. An officer would then request that the assistant state attorney subpoena the corresponding ISPs for the purpose of identifying the subscribers that were transmitting the illegal content.

17. In these cases, the subscribers were not notified by the ISPs that their identity was being subpoenaed because they could have deleted the images and destroyed the data.

18. After receiving the subscribers' identities, we would prepare a search warrant that would authorize us to enter the subscribers' dwelling and seize all of their computer devices.

19. I was directly involved in approximately 200 search warrants either by way of managing the process or performing it personally while at the Computer Crimes Unit.

20. I can recall only one instance in all the times that we executed a search warrant and seized computers where we did not find the items listed in the search warrant at the dwelling identified in the search warrant.

21. In that one instance, the Wi-Fi connection was not password protected, and the offender was a neighbor behind the residence.

22. I never came across a Wi-Fi hacker situation.

23. In my opinion, a child pornographer has a greater incentive to hack someone's Wi-Fi connection than a BitTorrent user because transmission of child pornography is a very serious crime with heavy criminal penalties, and many offenders can face life sentences if convicted.

24. I tested IPP International U.G.'s ("IPP") IP detection process.

25. To do so, I downloaded four public domain movies from the national archive.

26. I then encoded text into the videos, so that I would know whether someone that downloaded that particular movie downloaded the version of the movie that I created.

27. I then rented four virtual servers, each of which was connected to the Internet and used a unique IP addresses.

28. I then configured the servers so that all of them were running Windows 2008 server edition, and I put a different BitTorrent client onto each server.

29. A BitTorrent "client" is software that enables the BitTorrent protocol to work.

30. After installing the BitTorrent clients, I also installed Wireshark onto each server. "Wireshark" is a program that captures network traffic and creates PCAPs, just as TCP Dump, which IPP uses, does. A PCAP is like a video recording of all the incoming and outgoing transactions of a computer.

31. After installing Wireshark onto each of the servers, I transferred the movies from my local computer to the servers.

32. I then used the BitTorrent clients on each of the servers to make .torrent files. I uploaded these .torrent files onto various torrent websites.

33. I then informed IPP of the movie names. Thereafter, IPP sent me screen captures of the movies I had seeded.

34. The screen captures sent by IPP had my codes on them; thus, I knew that IPP had caught the movies I had seeded.

35. IPP also sent me additional data identifying the IP Address used by each of the four servers, and sent me PCAPs.

36. I reviewed IPP's PCAPs vis-à-vis the PCAP log files created by each of my test servers, and determined that IPP's PCAPs match my PCAPs. This could not have happened unless IPP's server was connected to the test server because the transactions would not match.

37. From this test, I concluded that IPP's software worked, and had a subpoena been issued for my IP addresses, it would have revealed my identity.

38. With regards to this case, I examined Defendant's hard drive images for any evidence of: (a) use of the BitTorrent protocol; (b) infringement of the copyrighted "X-Art" works owned by Plaintiff, Malibu Media, LLC ("Malibu Media"); (c) spoliation of evidence; and (d) suppression of evidence.

39. On December 26, 2014, I received a package from Tim Kiefer of D4 Data in Rochester, New York. Mr. Kiefer's package contained one Western Digital hard drive. The Western Digital Hard Drive contained two (2) EnCase images of computer devices listed as belonging to Defendant Jesse Raleigh ("Defendant"). *See* Paige Report, Exhibit A, p. 1. One (1) of the EnCase images was of Defendant's MacBook C02HW056DV31 ("MacBook Laptop No. 1") and the other Encase image was of Defendant's MacBook 340269NBATM ("MacBook

Laptop No. 2"). Lastly, the Western Digital Hard Drive contained two (2) Cellebrite iPad extractions.

40. Prior to examination, I was provided with a list of: (a) the torrent filenames for Plaintiff's copyrighted works infringed; and (b) the torrent filenames of numerous third party works that IPP detected were distributed through BitTorrent by a computer using Defendant's IP address ("Additional Evidence").

41. I conducted my examination of Defendant's computer devices using the forensic software EnCase Version 6 & 7 by Guidance Software ("EnCase") and Internet Evidence Finder by Magnet Forensics ("IEF").

42. The results of my examination are set forth in the Report of Findings ("Paige Report") attached hereto as Exhibit "A." I also exported supporting documentation contained in a .zip folder titled "Raleigh Final Report Case Files" attached hereto as Exhibit "B"

43. In sum, within Defendant's computer devices I discovered evidence which demonstrates: (a) BitTorrent use; and (b) the existence of other computer devices that have not been produced to me for examination. *See* Paige Report, Exhibit A.

DEFENDANT'S MACBOOK LAPTOP NO. 1

DEFENDANT'S MACBOOK LAPTOP NO. 1 CONTAINS EVIDENCE OF BITTORRENT USE

44. Using EnCase software a keyword search for "torrent" was conducted. *See* Paige Report, Exhibit A, p. 4. Upon examining the search hits I located a text file named "David_Cesolini_Chats.txt" which contained a discussion about torrents. *See* Paige Report, Exhibit A, p. 4; *See* Exhibit B. Further examination revealed that this chat and other files contained in a folder "Chinga_La_Migra_Dos" may be related to a hacking event that took place in 2011. *See* Paige Report, Exhibit A, p. 4. This computer contains the sensitive files released by

hacker(s) which contain individuals' personal information including social security, driver's license numbers, account passwords etc. *See* Paige Report, Exhibit A, p. 4. Because of the sensitive nature of this information, my report contains redacted screenshots to preserve the confidential information of listed third parties. *Id.*

45. I also discovered several other Adium, skype, and iMessage chats about BitTorrent, and torrents. *See* Paige Report, Exhibit A, p. 3; *See* Exhibit B.

46. I was also able to locate an "NFO" file. *Id.* NFO files are commonly associated with pirated files and are often included with the infringed files(s). *See* Paige Report, Exhibit A, p. 3

47. In my examination of Defendant's Macbook Laptop No. 1, I located two (2) Parallels Virtual Machines. *See* Paige Report, Exhibit A, p. 5. One was named Windows 7-0.hdd ("Windows 7-0") and the other was named Windows XP.hdd ("Windows XP"). *See* Paige Report, Exhibit A, p. 5; *See* Exhibit B.

48. A virtual machine is an emulation of a computer system which imitates the structure and functions of a real computer system. Virtual machines are created and operated using virtualization software. Simply put, these virtual machines needed to be examined independently, because they emulate an entire independent computer system.

49. Parallels Desktop software is hardware virtualization software for the MAC operating system. Parallels software allows the user to create and run virtual operating systems including Windows based operating systems on a MAC computer.

50. In this case the user was utilizing a Microsoft Windows XP virtual machine via the Parallels Software. *See* Paige Report, Exhibit A, p. 5. Using EnCase software I copied out the "Windows XP" virtual along with the companion configuration files to my local forensics

machine. *Id.* Using software "VMware vCenter Converter Standalone Client" I converted the image to a VMware virtual machine and loaded the image into IEF forensic software for processing and examination. *See* Paige Report, Exhibit A, p. 5. The same process was followed for the "Windows 7" Parallels virtual machine however the configurations appeared to be corrupt. *Id.* And, I was therefore unable to examine the "Windows 7" virtual machine.

51. Using IEF and EnCase software I located a BitTorrent client titled "uTorrent" on the "Windows XP" virtual machine and a LNK file in the start menu for the computer user "Jesse". *See* Paige Report, Exhibit A, p. 6.

DEFENDANT'S MACBOOK LAPTOP NO. 1 CONTAINS FOLDERS EVIDENCING THE EXISTENCE OF UNDISCLOSED STORAGE ON A LOCAL NETWORK AND CLOUD STORAGE SERVICE

52. Using EnCase and IEF software I searched for possible undisclosed network storage locations. *See* Paige Report, Exhibit A, p. 6.

53. In searching for possible undisclosed network storage locations, I discovered the "NetHood" folder. *Id.* The NetHood folder stores the path to the folder containing shortcuts to servers that the user has added to My Network Places. This indicates additional file storage somewhere on a local network. *Id.* IEF discovered locations on the network including "PSF" where folders are being accessed including "\\psf\Parallels Desktop" 7&8. *Id.* The Parallels Desktop folder 7&8 evinces the possible existence of other virtual machines or the storage of other various versions of Parallels software. *Id.* I exported IEF's complete list of Network Share Information and Shellbags to the final report case files. *See* Exhibit B.

54. Using IEF, I also located hundreds of "Cloud Services" related URLs (Web Addresses) relating to sites like Dropbox and Google Drive. *See* Paige Report, Exhibit A, p. 3. *See* Exhibit B.

55. The contents of these Cloud services have not been produced to me for examination.

DEFENDANT'S MACBOOK LAPTOP NO. 2

DEFENDANT'S MACBOOK LAPTOP NO. 2 CONTAINS EVIDENCE OF BITTORRENT USE

56. Using IEF I discovered evidence of BitTorrent use on Defendant's MacBook Laptop No. 2. Specifically, I discovered:

a. Several BitTorrent related website URLs pertaining to the website "The Pirate Bay." *See* Paige Report, Exhibit A, p. 8; *See* Exhibit B. The Pirate Bay is an online website which enables piracy of copyrighted works through its extensive index of torrent files;

b. The installation of a BitTorrent client titled "uTorrent" *See* Paige Report, Exhibit A, p. 8; and

c. Numerous music media files which have embedded metadata referencing "www.torrentazos.com" which suggests file origin from this website. *See* Paige Report, Exhibit A, p. 8. The website "www.torrentazos.com" contains illegally obtained computer media files.

UNDISCLOSED AND UNPRODUCED STORAGE DEVICES

DEFENDANT'S MACBOOK LAPTOP NO. 1 AND 2 CONTAIN SYSTEM LOG FILES EVIDENCING THE EXISTENCE OF UNDISCLOSED STORAGE DEVICES

57. Using EnCase software I conducted a keyword search of the "system.log" files located on both Defendants' MacBook Laptop No. 1 and No. 2 using the keyword "USBMSC". *See* Paige Report, Exhibit A, p. 10; *See* Exhibit B. I was able to locate and identify USB devices that were plugged into the two computer devices. *Id.*

58. As outlined in my report, I am able to conclude that a Western Digital MyBook Essentials External Hard Drive ("Western Digital Hard Drive") serial number "574D415A4139303734343136" was last accessed on December 2, 2014. *See* Paige Report, Exhibit A, p. 10; *See* Exhibit B.

59. Using EnCase software I conducted a keyword search for serial number "574D415A4139303734343136" pertaining to the Western Digital Hard Drive. *Id.* The results of this search prove that this device was plugged into both the MacBook Laptop No. 1 and MacBook Laptop No. 2 numerous times. *Id.*

60. The Western Digital Hard Drive was plugged into Defendant's MacBook Laptop No. 1 between July 10, 2013 and December 2, 2014. *See* Paige Report, Exhibit A, p. 11; *See* Exhibit B.

61. The Western Digital Hard Drive was plugged into Defendant's MacBook Laptop No. 2 between October 13, 2011 and February 17, 2014. *Id.*

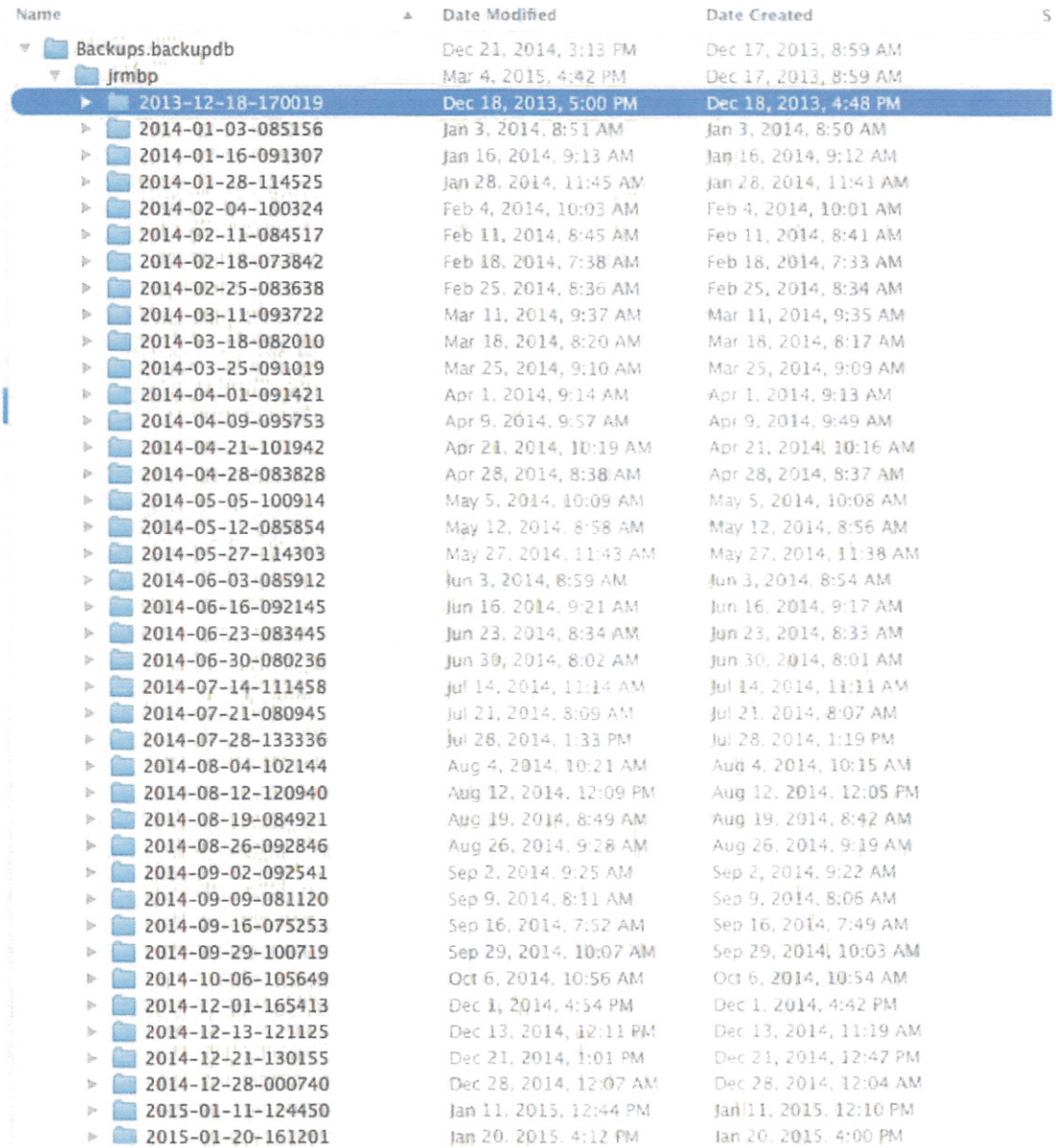
62. The foregoing proves the existence of a Western Digital Hard Drive and its consistent use in connection with Defendant's MacBook Laptop No. 1 and MacBook Laptop No. 2 for the past five years.

63. As of February 13, 2015, the Western Digital Hard Drive had not been produced to me for examination.

64. As outlined in my report, I was also able to locate a last know access date of October 15, 2014 for a Toshiba External Hard Drive. *See* Paige Report, Exhibit A, p. 13.

65. The Toshiba External Hard Drive has not been produced to me for examination.

75. The Western Digital Hard Drive contained 72 backup folders dated from December 18, 2013 to March 4, 2015. The below screen capture shows the backups in 2014 occurred on average 3-4 times a month. *See* Exhibit C, p. 2.



Name	Date Modified	Date Created	S
Backups.backupdb	Dec 21, 2014, 3:13 PM	Dec 17, 2013, 8:59 AM	
jrmbp	Mar 4, 2015, 4:42 PM	Dec 17, 2013, 8:59 AM	
2013-12-18-170019	Dec 18, 2013, 5:00 PM	Dec 18, 2013, 4:48 PM	
2014-01-03-085156	Jan 3, 2014, 8:51 AM	Jan 3, 2014, 8:50 AM	
2014-01-16-091307	Jan 16, 2014, 9:13 AM	Jan 16, 2014, 9:12 AM	
2014-01-28-114525	Jan 28, 2014, 11:45 AM	Jan 28, 2014, 11:41 AM	
2014-02-04-100324	Feb 4, 2014, 10:03 AM	Feb 4, 2014, 10:01 AM	
2014-02-11-084517	Feb 11, 2014, 8:45 AM	Feb 11, 2014, 8:41 AM	
2014-02-18-073842	Feb 18, 2014, 7:38 AM	Feb 18, 2014, 7:33 AM	
2014-02-25-083638	Feb 25, 2014, 8:36 AM	Feb 25, 2014, 8:34 AM	
2014-03-11-093722	Mar 11, 2014, 9:37 AM	Mar 11, 2014, 9:35 AM	
2014-03-18-082010	Mar 18, 2014, 8:20 AM	Mar 18, 2014, 8:17 AM	
2014-03-25-091019	Mar 25, 2014, 9:10 AM	Mar 25, 2014, 9:09 AM	
2014-04-01-091421	Apr 1, 2014, 9:14 AM	Apr 1, 2014, 9:13 AM	
2014-04-09-095753	Apr 9, 2014, 9:57 AM	Apr 9, 2014, 9:49 AM	
2014-04-21-101942	Apr 21, 2014, 10:19 AM	Apr 21, 2014, 10:16 AM	
2014-04-28-083828	Apr 28, 2014, 8:38 AM	Apr 28, 2014, 8:37 AM	
2014-05-05-100914	May 5, 2014, 10:09 AM	May 5, 2014, 10:08 AM	
2014-05-12-085854	May 12, 2014, 8:58 AM	May 12, 2014, 8:56 AM	
2014-05-27-114303	May 27, 2014, 11:43 AM	May 27, 2014, 11:38 AM	
2014-06-03-085912	Jun 3, 2014, 8:59 AM	Jun 3, 2014, 8:54 AM	
2014-06-16-092145	Jun 16, 2014, 9:21 AM	Jun 16, 2014, 9:17 AM	
2014-06-23-083445	Jun 23, 2014, 8:34 AM	Jun 23, 2014, 8:33 AM	
2014-06-30-080236	Jun 30, 2014, 8:02 AM	Jun 30, 2014, 8:01 AM	
2014-07-14-111458	Jul 14, 2014, 11:14 AM	Jul 14, 2014, 11:11 AM	
2014-07-21-080945	Jul 21, 2014, 8:09 AM	Jul 21, 2014, 8:07 AM	
2014-07-28-133336	Jul 28, 2014, 1:33 PM	Jul 28, 2014, 1:19 PM	
2014-08-04-102144	Aug 4, 2014, 10:21 AM	Aug 4, 2014, 10:15 AM	
2014-08-12-120940	Aug 12, 2014, 12:09 PM	Aug 12, 2014, 12:05 PM	
2014-08-19-084921	Aug 19, 2014, 8:49 AM	Aug 19, 2014, 8:42 AM	
2014-08-26-092846	Aug 26, 2014, 9:28 AM	Aug 26, 2014, 9:19 AM	
2014-09-02-092541	Sep 2, 2014, 9:25 AM	Sep 2, 2014, 9:22 AM	
2014-09-09-081120	Sep 9, 2014, 8:11 AM	Sep 9, 2014, 8:06 AM	
2014-09-16-075253	Sep 16, 2014, 7:52 AM	Sep 16, 2014, 7:49 AM	
2014-09-29-100719	Sep 29, 2014, 10:07 AM	Sep 29, 2014, 10:03 AM	
2014-10-06-105649	Oct 6, 2014, 10:56 AM	Oct 6, 2014, 10:54 AM	
2014-12-01-165413	Dec 1, 2014, 4:54 PM	Dec 1, 2014, 4:42 PM	
2014-12-13-121125	Dec 13, 2014, 12:11 PM	Dec 13, 2014, 11:19 AM	
2014-12-21-130155	Dec 21, 2014, 1:01 PM	Dec 21, 2014, 12:47 PM	
2014-12-28-000740	Dec 28, 2014, 12:07 AM	Dec 28, 2014, 12:04 AM	
2015-01-11-124450	Jan 11, 2015, 12:44 PM	Jan 11, 2015, 12:10 PM	
2015-01-20-161201	Jan 20, 2015, 4:12 PM	Jan 20, 2015, 4:00 PM	

72. Defendant provided me with the password "dontbeafuckingprickman15423" which successfully unlocked the volume. *See* Exhibit C, p. 2.

73. Using BlackLight forensic software I processed the contents of the drive and was able to view the folder structure. The folder structure revealed the drive was used as a "backup drive" through the use of software titled "Time Machine". *Id.*

74. Time Machine is backup software that creates backups of files which can be restored at a later date. Time Machine keeps all the backups stored until the disk (on which the backup is stored) becomes full. Once the disk is full, the oldest backups are deleted. *See* Exhibit C, p. 3.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

DEFENDANT'S WESTERN DIGITAL HARD DRIVE

AN EXTENSIVE AMOUNT OF BACKUP ACTIVITY OCCURRED SHORTLY BEFORE PRODUCTION OF DEFENDANT'S WESTERN DIGITAL HARD DRIVE

66. On March 6, 2015, I received a UPS package with the tracking number 1Z51708E0263740194 from Defendant, Jesse Raleigh. The package contained a power supply cord and one Western Digital external 2TB My Book hard disk drive, serial number 574D415A4139303734343136 ("Western Digital Hard Drive"). *See* Paige Report on Western Digital Hard Drive, attached hereto as Exhibit C.

67. Based on the matching serial numbers, I concluded that this was the exact Western Digital Hard Drive discussed in paragraphs 58-63 of this declaration, which was not initially produced to me for examination.

68. To create a forensically sound image of the Western Digital Hard Drive, I connected it to a Tableau TD3 forensic device. *See* Exhibit C, p. 2.

69. The image files were then loaded into EnCase forensic software which verified that the files contained no errors. *Id.*

70. Once loaded into EnCase, I discovered that the hard drive contained a FileVault2 encrypted volume. In order to read the encrypted volume I connected the Western Digital Hard Drive back to the Tableau TD3 device and made a RAW image of the Western Digital Hard Drive onto a 3TB wiped hard drive ("Cloned Hard Drive"). This Cloned Hard Drive was then connected to a Tableau T35u USB3 write blocker which was then connected to my MacBook Pro forensic computer. *Id.*

71. Once I connected the Cloned Hard Drive, I was prompted to enter the password for the encrypted volume titled "JR Backup". *Id.*

76. This trend continued until March 2015 when a total of twenty-four (24) backups were performed that month. Of these twenty-four (24) backups, sixteen (16) occurred the same day the Western Digital Hard Drive was shipped to my office for analysis (March 4, 2015). *See* Exhibit C, p. 2.

2015-02-03-181234	Feb 3, 2015, 6:12 PM	Feb 3, 2015, 5:50 PM
2015-02-04-004928	Feb 4, 2015, 12:49 AM	Feb 4, 2015, 12:47 AM
2015-02-05-000003	Feb 5, 2015, 12:00 AM	Feb 4, 2015, 11:59 PM
2015-02-18-163722	Feb 18, 2015, 4:37 PM	Feb 18, 2015, 3:09 PM
2015-02-19-000006	Feb 19, 2015, 12:00 AM	Feb 18, 2015, 11:58 PM
2015-02-20-005805	Feb 20, 2015, 12:58 AM	Feb 20, 2015, 12:53 AM
2015-02-21-003520	Feb 21, 2015, 12:35 AM	Feb 21, 2015, 12:33 AM
2015-02-22-113409	Feb 22, 2015, 11:34 AM	Feb 22, 2015, 11:29 AM
2015-03-02-095822	Mar 2, 2015, 9:58 AM	Mar 2, 2015, 8:05 AM
2015-03-03-005515	Mar 3, 2015, 12:55 AM	Mar 3, 2015, 12:53 AM
2015-03-03-164809	Mar 3, 2015, 4:48 PM	Mar 3, 2015, 4:39 PM
2015-03-03-175825	Mar 3, 2015, 5:58 PM	Mar 3, 2015, 5:52 PM
2015-03-03-190622	Mar 3, 2015, 7:06 PM	Mar 3, 2015, 7:00 PM
2015-03-03-204904	Mar 3, 2015, 8:49 PM	Mar 3, 2015, 8:10 PM
2015-03-03-215558	Mar 3, 2015, 9:55 PM	Mar 3, 2015, 9:51 PM
2015-03-03-225949	Mar 3, 2015, 10:59 PM	Mar 3, 2015, 10:58 PM
2015-03-04-000209	Mar 4, 2015, 12:02 AM	Mar 4, 2015, 12:01 AM
2015-03-04-010526	Mar 4, 2015, 1:05 AM	Mar 4, 2015, 1:03 AM
2015-03-04-020806	Mar 4, 2015, 2:08 AM	Mar 4, 2015, 2:06 AM
2015-03-04-031102	Mar 4, 2015, 3:11 AM	Mar 4, 2015, 3:09 AM
2015-03-04-041437	Mar 4, 2015, 4:14 AM	Mar 4, 2015, 4:12 AM
2015-03-04-051809	Mar 4, 2015, 5:18 AM	Mar 4, 2015, 5:16 AM
2015-03-04-062030	Mar 4, 2015, 6:20 AM	Mar 4, 2015, 6:19 AM
2015-03-04-072629	Mar 4, 2015, 7:26 AM	Mar 4, 2015, 7:22 AM
2015-03-04-083827	Mar 4, 2015, 8:38 AM	Mar 4, 2015, 8:28 AM
2015-03-04-094651	Mar 4, 2015, 9:46 AM	Mar 4, 2015, 9:41 AM
2015-03-04-105101	Mar 4, 2015, 10:51 AM	Mar 4, 2015, 10:48 AM
2015-03-04-115730	Mar 4, 2015, 11:57 AM	Mar 4, 2015, 11:53 AM
2015-03-04-130501	Mar 4, 2015, 1:05 PM	Mar 4, 2015, 1:00 PM
2015-03-04-141504	Mar 4, 2015, 2:15 PM	Mar 4, 2015, 2:07 PM
2015-03-04-152329	Mar 4, 2015, 3:23 PM	Mar 4, 2015, 3:17 PM
2015-03-04-164028	Mar 4, 2015, 4:40 PM	Mar 4, 2015, 4:24 PM

77. In fact, between March 3, 2015 at 4:39 PM and March 4, 2015 at 4:44 PM, Defendant's backed up his computer every single hour.

78. According to UPS records, on March 4, 2015 at 6:20 PM, Defendant shipped his hard drive. *See* UPS Tracking Records, attached hereto as Exhibit D.

79. During my search of this hard drive, I also discovered various BitTorrent files. *See* Exhibit C, p. 4-18.

80. I am paid on an hourly basis by Malibu Media, LLC, at the rate of $325.00 per hour for pre-trial investigative work, although the fee increases if I am required to testify at trial.

FURTHER DECLARANT SAYETH NAUGHT.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury that the foregoing is true and correct.

Executed on this 20th day of March, 2015.

By: _____
PATRICK PAIGE